A Value Analysis of Machine Learning-based Usable Privacy

IFIP Working Group 8.2
OASIS Pre-ICIS 2022 Workshop

Jenni Reuben
Totalförsvarets forskningsinstitut (FOI)
jenni.reuben@foi.se

Ala Sarah Alaqra
Karlstad University
as.alaqra@kau.se

Abstract

With the ubiquitous presence of machine learning based decision making in the digitalization of various processes, workflows and solutions across every functional area of our society, it is important to understand the value of such systems. Especially, to understand the value of them in the light of end user's privacy because machine learning programs learn accurate inferences by inductively extracting information from various pieces of data. We aim to study the relationship of a machine learning based detection of anti-privacy user interface design patterns (dark patterns) and self-determination of the end users, in order to analyze the value of the machine learning technology. To this end, we are in the process of i) investigating the perspectives of practitioners in the field of machine learning-based usable privacy and ii) developing a machine learning program that detects dark patterns in website's consent form designs. Following which, we plan to conduct user studies to empirically study end users perspectives for example on machine learning assisted decision on one's online privacy.

Keywords (Required)

Machine learning, usable privacy, dark patterns, self-determination, detection

Research Project Description

Advances in computation and storage capabilities of computers have revived the field of Machine Learning (ML). Now machine learning applications are transforming the technological landscape in every domain of our functional society, for example in domains such as e-commerce, health care, financial management, etc. The increasing and rapid transformation of our society's technological space raises many fundamental questions such as the value of these intelligence systems in the light of our autonomy, transparency aspects of these systems, etc. The value of machine learning methods and technologies is often put to question when it comes to end-users' privacy. However, research concerning privacy of machine learning models and applications often focuses on information leakage in the machine learning pipeline, the relationship structure between machine learning systems and legal privacy principles is often overlooked. Therefore the primary aim of the work is to study the nature of the relationship between the value of machine learning and self-determination of end users. In particular, we investigate the use of machine learning for determining anti-privacy dark patterns in user interfaces, in order to understand the trade-off between ML's utility and the ethical concern such as self-determination. Anti-privacy dark patterns are UI design elements (e.g., text of a cookie consent notice) that online service providers use to trick their users into engaging with their system in ways that the users otherwise would not engage consciously, had it not been for the dark patterns. The analysis of machine learning features that characterizes dark patterns in textual design elements, employs our exploration of assessing ML-based usable privacy approaches beginning with investigating perspectives of relevant stakeholders in the field of applied cases. We follow that with the implementation of a machine learning dark pattern detection program and user studies for evaluating the utility of ML-based privacy applications and self-determination of user's privacy . We see our work to set the basis for future studies investigating usability of ML-based privacy.